



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/893,501	06/29/2001	Todd Flemming	26509U	6332
20529 7590 04/03/2006				
NATH & ASSOCIATES 112 South West Street Alexandria, VA 22314				
EXAMINER SHIFERAW, ELENI A				
ART UNIT			PAPER NUMBER	
2136				

DATE MAILED: 04/03/2006

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary

Application No.

09/893,501

Applicant(s)

FLEMMING, TODD

Examiner

Eleni A. Shiferaw

Art Unit

2136

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
 - If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
 - Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133).
- Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

- 1) ☒ Responsive to communication(s) filed on 30 January 2006.
- 2a) ☐ This action is **FINAL**.
- 2b) ☒ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

- 4) ☒ Claim(s) 1-3, 5, 7-9, 12-17 and 19-29 is/are pending in the application.
- 4a) Of the above claim(s) _____ is/are withdrawn from consideration.
- 5) ☐ Claim(s) _____ is/are allowed.
- 6) ☒ Claim(s) 1-3, 5, 7-9, 12-17 and 19-29 is/are rejected.
- 7) ☐ Claim(s) _____ is/are objected to.
- 8) ☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

- 9) ☐ The specification is objected to by the Examiner.
- 10) ☐ The drawing(s) filed on _____ is/are: a) ☐ accepted or b) ☐ objected to by the Examiner.
- Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).
- Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

- 12) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☐ All b) ☐ Some * c) ☐ None of:
1. ☐ Certified copies of the priority documents have been received.
2. ☐ Certified copies of the priority documents have been received in Application No. _____.
3. ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

- 1) ☒ Notice of References Cited (PTO-892)
- 2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
- 3) ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08)
- Paper No(s)/Mail Date _____

- 4) ☐ Interview Summary (PTO-413)
- Paper No(s)/Mail Date. _____
- 5) ☐ Notice of Informal Patent Application (PTO-152)
- 6) ☐ Other: _____

DETAILED ACTION

Continued Examination Under 37 CFR 1.114

1. A request for continued examination under 37 CFR 1.114, including the fee set forth in 37 CFR 1.17(e), was filed in this application after final rejection. Since this application is eligible for continued examination under 37 CFR 1.114, and the fee set forth in 37 CFR 1.17(e) has been timely paid, the finality of the previous Office action has been withdrawn pursuant to 37 CFR 1.114. Applicant's submission filed on 01/30/2006 has been entered.

Claim Rejections - 35 USC § 102

2. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

A person shall be entitled to a patent unless –

(e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

3. Claims 1, 12 and 20 rejected under 35 U.S.C. 102(e) as being anticipated by Mimura et al. USPN 6,747,564 B1.

a physical asset protection module that provides physical protection for said asset by triggering a user status change upon valid entry or exit through a door of a building (fig. 1 & 8 and col. 4 lines 23-42; *smart card door authentication*);

an information asset protection module that provides information security protection for said asset (col. 4 lines 22-65; *bank door and bank user database, that stores important customer's information, authentication*);

Application/Control Number: 09/893,501
Art Unit: 2136

an integrator that performs an integration of said physical asset protection module and said information asset protection module, wherein said system is one of in a hosted environment and at said asset, the integrator providing integration of the physical protection and information from the information asset protection module to grant rights to the information systems based on physical access, or independently of physical access, wherein the information asset protection reflects the user status change updated to reflect changes in security access requirements (col. 5 lines 50-col. 7 lines 55; *building authentication information result fails access to the computer database log-on is denied i.e. smart card door authentication is integrated with computer database/application authentication*); and

transmitter for maintaining information asset protection by denying access to the information asset in the hosted environment when there is a breach of the physical asset protection (col. 7 lines 1-65; *if the receiving door authentication fingerprint verification result as a success or failure and granting/denying computer application access based on the received verification result*).

Claim Rejections - 35 USC § 103

4. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

5. Claims 1, 12 and 20 are rejected under 35 U.S.C. 103(a) as being unpatentable over Claus et al. in view of Monroe Pub. No.: US 2003/0025599 A1.

Regarding claims 1, 12, and 20, Claus et al. a method/system for protecting an asset, comprising:

a physical asset protection module that provides physical protection for said asset by triggering a user status change upon valid entry or exit through a door of a building (fig. 7);

an information asset protection module that provides information security protection for said asset (col. 9 lines 48-65; *authenticating ... granting access... to information in a computer...*);

an integrator that performs an integration of said physical asset protection module and said information asset protection module, wherein said system is one of in a hosted environment and at said asset, the integrator providing integration of the physical protection and information from the information asset protection module to grant rights to the information systems based on physical access, or independently of physical access (col. 11 lines 17-col. 12 lines 4 and col. 3 lines 33-52; *physical asset protection (smart card authentication to open a building door)...and computer information resource protection are performed in a single user smart card authentication and/or multiple different authentication is performed in using a single smart card to grant access, to building door... computer information*); and

transmitter for maintaining information asset protection by denying access to the information asset in the hosted environment when there is a breach of the physical asset protection (col. 10 lines 1-34; *when smart card authentication is not valid access to the computer application is denied*).

Claus et al. fails to disclose wherein the information asset protection reflects the user status change updated to reflect changes in security access requirements.

Application/Control Number: 09/893,501
Art Unit: 2136

However Monroe discloses wherein the information asset protection reflects the user status change updated to reflect changes in security access requirements (par. 0048-0050; *a user smart card is authenticated to open a door and user's status change/personal attempts to gain access through an access control system and each users movement is logged/updated to reflect changes n security access requirements*).

Therefore it would have been obvious to one having ordinary skill in the art at the time of the invention was made to employ the teachings of Monroe within the system of Claus et al. because it would further monitor and/or authenticate the user. One would have been motivated to do so because it would allow further security.

6. Claims 1-3, 5, 7-9, 12-17, and 19 are rejected under 35 U.S.C. 103(a) as being unpatentable over Baird, III et al. (Baird, Patent No.: US 6,732,278 B2) in view of Monroe Pub. No.: US 2003/0025599 A1.

As per claims 1 and 12, Baird teaches a method of protecting an asset of an information and/or physical type, comprising:

- providing processor-based physical asset protection (Baird Col. 16 lines 39-65;
- processor-based smart card is provided to protect data and for access control);
- providing processor-based information asset protection (Baird Col. 12 lines 15-col. 13 lines 5; password is used to access the site and data is encrypted to protect asset);
- integrating said processor-based physical asset protection and said processor-based information asset protection in a hosted environment (Col. 16 lines 61-col. 17 lines 67, and

Application/Control Number: 09/893,501

Art Unit: 2136

Abstract; process-based smart card and information asset protection is integrated by authenticating user's password and biometric data stored in the smart card.); and transmitting a breach of physical asset protection in the hosted environment such that information asset protections maintained by denying access thereto (fig. 7 element 605, and 607, col. 18 lines 34-37 and col. 20 lines 21-26).

Baird teaches triggering a user status change upon valid entry or exit through a device (Baird col. 8 lines 16-21; triggering a user password changes upon valid entry denying access to the changed (old password)), Baird does not explicitly teach triggering a user status change upon valid entry or exit through a *door of a building*.

However **Monroe** discloses triggering a user status change upon valid entry or exit through a door of a building (0048-0070).

Therefore it would have been obvious to one having ordinary skill in the art at time of the invention was made to combine the teachings of Monroe within the system of Baird because they are analogous in access control (claim 59). One skilled in the art would have been motivated to combine the teachings of Monroe within the system of Baird because it would further control an unauthorized access from entering a building door by updating a users database of any changes.

As per claim 2, Baird and Monroe teach all the subject matter as described above. In addition, Baird teaches the method, said integrating further comprising providing, maintaining and operating a software application that integrates said physical asset protection (Baird Col. 5 lines 33-42) and said information asset protection in said hosted environment in accordance with user instructions (Baird Abstract).

Application/Control Number: 09/893,501
Art Unit: 2136

As per claim 3, Baird and Monroe teach all the subject matter as described above. In addition, Baird teaches the method, further comprising:

registering a user by storing user information (Baird Col. 7 lines 19-33);

authenticating a user by comparing at least one user characteristic from said user information with a third-party database (Baird Col. 7 lines 63-col. 8 lines 21);

comparing a current asset use pattern with a historical asset use pattern for said user to detect anomalous usage (Baird Col. 12 lines 10-28);

updating said historical use pattern on the basis of said current use pattern (Baird Col. 8 lines 1-21);

taking a corrective action, wherein a first corrective action is taken if said authenticating step generates a non-authenticated user output and a second corrective action is taken if anomalous usage is detected during said comparing step (Baird Fig. 7 No. 604, 606; if invalid input entered the corrective action is taken back to requesting a user to enter password and biometric data again); and

wherein said authenticating and comparing steps provide physical asset protection and information asset protection and are performed in said hosted environment (Baird Abstract).

As per claim 5, Baird and Monroe teach all the subject matter as described above. In addition, Baird teaches the method, further comprising:

registering a visitor by providing initial visitor information (Baird Col. 7 lines 19-33);

comparing said initial visitor information with a third-party database to determine if said registered visitor is entitled to access to said asset (Baird Col. 7 lines 63-col. 8 lines 21); and receiving said registered visitor in an authentication area (Baird Col. 8 lines 22-32); checking a match of said registered visitor with a physical entity (Baird Col. 14 lines 36-44, col. 17 lines 59-col. 18 lines 4);

regulating entry on the basis of said checking and comparing steps, wherein said registered visitor is denied access if said registered visitor does not match said physical entity, or said comparing step indicates that said visitor does not have access to said asset (Baird Col. 17 lines 1-27); and

wherein at least one of said comparing step, said receiving step and said checking step provide physical asset protection and information asset protection (Baird Abstract).

As per claim 7, Baird and Monroe teach all the subject matter as described above. In addition, Baird teaches the method, wherein one of said receiving and said comparing step comprises applying biometrics to control access for said user (Baird Col. 8 lines 1-21).

As per claim 8, Baird and Monroe teach all the subject matter as described above. In addition, Baird teaches the method, wherein said biometrics comprises one of scanning and testing a target tissue of said visitor's body (Baird Col. 17 lines 28-31).

As per claim 9, Baird and Monroe teach all the subject matter as described above. In addition, Baird teaches the method, wherein said physical asset protection comprises securing ingress and

egress areas for a location protected by a physical barrier (Baird Col. 2 lines 1-17; biometric smart card is used to gain access to gain access to protected data).

As per claim 13, Baird and Monroe teach all the subject matter as described above. In addition, Baird teaches the asset protection system, further comprising:

a user tracking system that authenticates a user as a registered user and provides physical access and information access to said asset in accordance with historical use patterns of said user for said asset, wherein said user tracking system updates said historical use patterns in accordance with a current use pattern of said user (Baird Col. 19 lines 36-50, Fig. 7 No. 604, and 606).

As per claim 14, Baird and Monroe teach all the subject matter as described above. In addition, Baird teaches the asset protection system, said historical use patterns comprising at least one of frequency, type and time duration (Baird Col. 19 lines 36-50).

As per claim 15, Baird and Monroe teach all the subject matter as described above. In addition, Baird teaches the asset protection system, further comprising a visitor tracking system that authenticates a registered visitor that has not been barred from accessing said asset, and allows access in accordance with reception authentication process (Baird Col. 19 lines 36-50).

As per claim 16, Baird and Monroe teach all the subject matter as described above. In addition, Baird teaches the asset protection system, further comprising a biometrics authentication

Application/Control Number: 09/893,501

Art Unit: 2136

subsystem that uses physical data of said visitor to allow said access (Baird Col. 8 lines 1-21).

As per claim 17, Baird and Monroe teach all the subject matter as described above. In addition, Baird teaches the asset protection system, wherein said physical data comprises a test data portion of said visitor's body (Baird Col. 17 lines 28-31).

As per claim 19, Baird and Monroe teach all the subject matter as described above. In addition, Baird teaches the asset protection system, wherein said integration is performed in response to an instruction to develop, maintain and operate a computer application to protect said asset (Baird Abstract).

7. Claims 20-29 are rejected under 35 U.S.C. 103(a) as being unpatentable over Baird, III et al. (Baird, Patent No.: US 6,732,278 B2) in view of Boate et al. (Boate Pub. No.: US 2002/0104006 A1) and Monroe Pub. No.: US 2003/0025599 A1.

As per claim 20, Baird teaches a method of providing asset security protection, comprising:
hosted environment indicative of asset access, wherein protection of physical and information characteristics of said asset is integrated in said hosted environment (Baird Abstract; access to the device is granted after authentication process during which a user password and biometric are provided to the device),

Application/Control Number: 09/893,501
Art Unit: 2136

Baird does not explicitly teach transmitting and receiving a first and second signals respectively to a hosted environment, said first signal comprising user registration characteristics,

However **Boate et al.** teaches transmitting and receiving a signal to a host environment (Boate Fig. 4a) and new user registration (Boate Page 5 par. 0036)

Therefore it would have been obvious to one having ordinary skill in the art at the time the invention was made to employ the teachings of Boate with in the system of Baird because it would allow a secure authentication of an individual and access control to components of the computer network (Boate Page 1 par. 0001) by transmitting signals to the hosted environment and receiving signals from the hosted environment.

Baird and Boate do not explicitly teach triggering a user status change upon valid entry or exit through a *door of a building*.

However **Monroe** discloses triggering a user status change upon valid entry or exit through a door of a building (0048-0070).

Therefore it would have been obvious to one having ordinary skill in the art at time of the invention was made to combine the teachings of Monroe within the combination system of Baird and Boate because they are analogous in access control (claim 59). One skilled in the art would have been motivated to combine the teachings of Monroe within the system of Baird because it would further control an unauthorized access from entering a building door by updating a users database of any changes.

As per claim 21, Baird, Boate, and Monroe teach all the subject matter as described above. In addition Boate teaches the method, wherein said transmitting comprises:

providing user registration information to said hosted environment (Boate Page 5 par. 0036); and

processing at said hosted environment said user information to generate said second signal (Boate Page 5 par. 0036) The rationale for combining are the same as claim 20 above.

As per claim 22, Baird, Boate, and Monroe teach all the subject matter as described above. In addition Boate teaches wherein said receiving comprises receiving an access decision from said hosted environment, said decision being in accordance with biometrics of a user (Boate Page 4 par. 0032) The rationale for combining are the same as claim 20 above.

As per claim 23, Baird, Boate, and Monroe teach all the subject matter as described above. In addition Boate teaches further comprising comparing said user information to a third-party database to generate an authentication output as said second signal (Boate Page 6 par. 0045) The rationale for combining are the same as claim 20 above.

As per claim 24, Baird, Boate, and Monroe teach all the subject matter as described above. In addition Boate teaches further comprising:

entering credentials of a user into an access database in said hosted environment to enroll said user (Boate Page 5 par. 0036); and

Application/Control Number: 09/893,501

Art Unit: 2136

outputting an identification object in accordance with said credentials, wherein unauthorized access is denied by said hosted environment (Boate Page 4 par. 0034, Fig. 4B; access refusal message) Therefore it would have been obvious to one having ordinary skill in the art at the time of the invention to combine the teachings of Boate with in the system of Baird because it would register users information to enroll and would also inform users by their identification when the access is denied or accepted.

As per claim 25, Baird, Boate, and Monroe teach all the subject matter as described above. In addition Boate teaches said entering:

providing an authorized operator with permission to at least one of alter and append said access database (Boate Page 4 par. 0034);

obtaining a biometric from said user and searching for said biometric in said access database to generate a search result, wherein said biometric and credential data is added to said access database if said search result indicates an absence of said biometric (Boate Page 5 par. 0036), and if said search result indicates a presence of said biometric in said access database, one of verifying said credential data if said user is authentic and denying access to said user if said user is not authentic, in accordance with said biometric (Boate Page 5 par. 0039, page 6 par. 0045);

denying access to said user if said user appears in a barred user database (Boate Fig. 4C; message indicating refusal to logon);

Application/Control Number: 09/893,501

Art Unit: 2136

determining if a photo of said user is in said hosted environment, wherein a digital image is imported to generate said photo if said photo is not present in said hosted environment (Boate Page 4 par. 0032);

verifying that said photo represents said new user (Boate Page 5 par. 0036, page 6 par. 0045);

providing additional user information and user access privileges to said hosted environment (Boate Page 5 par. 0036); and

generating said identification object having a predetermined layout, said identification object comprising an encrypted three-dimensional barcode in accordance with said biometric and said credential data (Boate Page 5 par. 0036; user is handed a personal identification device that has biometric data, public key and private key) The rationale for combining are the same as claim 20 above.

As per claim 26, Baird, Boate, and Monroe teach all the subject matter as described above. In addition Boate teaches said outputting comprising: receiving said identification object from said hosted environment and producing a copy of said identification object; said user verifying integrity of said biometric, said photo and said credentials; and distributing said identification object to said user (Boate Page 5 par. 0036) The rationale for combining are the same as claim 24 above.

As per claim 27, Baird, Boate, and Monroe teach all the subject matter as described above. In addition Boate teaches, wherein said identification object is produced by printing an

Application/Control Number: 09/893,501

Art Unit: 2136

identification badge (Boate Page 5 par. 0036; personal digital identification device reads on identification badge) Therefore it would have been obvious to one having ordinary skill in the art at the time of the invention to combine the teachings of Boate with in the system of Baird because it would authenticate and integrate a users identity by password and biometric data.

As per claim 28, Baird, Boate, and Monroe teach all the subject matter as described above. In addition Boate teaches wherein said biometric comprises a scan of a biological target tissue (Boate Page 6 par. 0045). The rational for combining are the same as claim 27 above.

As per claim 29, Baird, Boate, and Monroe teach all the subject matter as described above. In addition Boate teaches, wherein said target tissue comprises at least one of finger, hand and eye parameter (Boate Page 6 par. 45). The rational for combining are the same as claim 27 above.

Conclusion

8. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Eleni A. Shiferaw whose telephone number is 571-272-3867. The examiner can normally be reached on Mon-Fri 8:00am-5:00pm.


If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz R. Sheikh can be reached on 571-272-3795. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

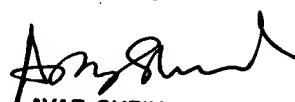
Application/Control Number: 09/893,501

Art Unit: 2136

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

E.S.


March 28, 2006


AYAZ SHEIKH
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100